UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/779,862	02/18/2004	Roberg Skog	4147-64	6213

23117 7590 10/22/2007
NIXON & VANDERHYE, PC
901 NORTH GLEBE ROAD, 11TH FLOOR
ARLINGTON, VA 22203

EXAMINER	
SIMITOSKI, MICHAEL J	

ART UNIT	PAPER NUMBER
2134	

MAIL DATE	DELIVERY MODE
10/22/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	**Application No.** 10/779,862	**Applicant(s)** SKOG ET AL.	
	Examiner Michael J. Simitoski	**Art Unit** 2134	

-- ***The MAILING DATE of this communication appears on the cover sheet with the correspondence address*** --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *18 February 2004*.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-21* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,2,4-10,12,13,15-19 and 21* is/are rejected.

7)☒ Claim(s) *3,11,14 and 20* is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *18 February 2004* is/are: a)☒ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)□ Some * c)□ None of:

1.☒ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date *2/18/2004*.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application

6) □ Other: _____.

DETAILED ACTION

1. The IDS of 2/18/2004 was received and considered.

2. Claims 1-21 are pending.

Priority

3. Receipt is acknowledged of papers submitted under 35 U.S.C. 119(a)-(d), which papers have been placed of record in the file.

Specification

4. The use of the trademark Sony Ericsson has been noted in this application.. It should be capitalized wherever it appears and be accompanied by the generic terminology.

Although the use of trademarks is permissible in patent applications, the proprietary nature of the marks should be respected and every effort made to prevent their use in any manner which might adversely affect their validity as trademarks.

Claim Objections

5. Claims 12-15 & 17 are objected to because of the following informalities:

a. Regarding claim 12, line 8, "tamper-resistant" should be replaced with "a tamper-resistant". Claims 13-15 are objected to based on their dependence on claim 12.

b. Regarding claim 17, line 6, "signature generator" should be replaced with "a signature generator".

6. Appropriate correction is required.

Claim Rejections - 35 USC § 102

7. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

8. Claims 1-2, 4-9, 12-13, 15-17, 19 & 21 are rejected under 35 U.S.C. 102(b) as being anticipated by "HTTP Authentication: Basic and Digest Access Authentication" by Franks et al. (**Franks**).

Regarding claim 1, Franks discloses a method for device-type authentication in a communications system comprising the steps of providing, in a first device (client, p. 11, §3.2.2, ¶1) connected to said communications system (communication system through which the client requests, p. 11, §3.2.2, ¶1 and the server receives requests, p. 8, §3.2.1, ¶1), first header information (components 'username|realm|nonce|digest-uri', p. 11, §3.2.2) of a communication message (HTTP request, p. 6, §3.1.1, ¶1, p. 7, §3.2.1, ¶1 & p. 11, §3.2.2, ¶1), said first header information being related with a device-type associated commitment (including the username in components 'username|realm|nonce|digest-uri', p. 11, §3.2.2, shows the device is associated with the user, p. 11, §3.2.2, ¶1), tamper-resistantly (using a hash function to create a signature is tamper resistant because to create the hash, the password must be known) creating a first signature (response, which comprises H(H(A1), unq(nonce-value);H(A2)), where A1 comprises unq(username):realm:password and A2 comprises the uri, p. 11, §3.2.2, p. 13, §3.2.2.1-3.2.2.2 & p. 14, §3.2.2.3) in said first device (client) based on at least tamper-resistant device-type specific information of said first device (A1, which is a hash function on at least a username and password, see definition of A1 on p. 13, §3.2.2.2), providing, in said first device (client), second header information (Authorization header, p. 11, §3.2.2, ¶1) of said communication message (HTTP request, p. 11, §3.2.2, ¶1) comprising said signature (the request contains the response, see §3.2.2, definition of digest-response), communicating said communication message (HTTP request) to a second device (server) connected to said communication system (HTTP request with authorization header is sent to server, p. 17, §3.3, ¶1), and authenticating said first header information ('username|realm|nonce|digest-uri', p. 11, §3.2.2) by verifying said first signature (response) after said communication step (server performs the same digest operation performed by the client, and compares the result to the given request-digest value, p. 17, §3.3, ¶1).

Regarding claim 2, Franks discloses wherein said communication system is based on a transfer protocol selected from the group of HyperText Transfer Protocol (HTTP/1.0, p. 6, §3.1.1, ¶1).

Regarding claim 4, Franks discloses wherein said first device is a user terminal (receives user's username and password, p. 8, §3.2.1, definition of 'realm').

Regarding claim 5, Franks discloses wherein said second device is a server (server, p. 17, §3.3, ¶1).

Regarding claim 6, Franks discloses wherein said device-type specific information (A1, which is a hash function on username and password, see definition of A1 on p. 13, §3.2.2.2) comprises a definition of an algorithm according to which said signature is to be created (hashing algorithm, p. 13, §3.2.2.2).

Regarding claim 7, Franks discloses wherein said device-type specific information (in this case, the device-type specific information, which is tamper-resistant/hashed to form the response/request-digest, see p. 13, §3.2.2.1, can also be the nonce value, which is shown to be based in part on the client's IP address, p. 22, §4.5, ¶2, the nonce also included in the values hashed to create the response/request-digest, see definition of request-digest, p. 13, §3.2.2.1) being a data string unique for each particular device type (unique to each device).

Regarding claim 8, Franks discloses wherein said step of creating a signature (response, which comprises H(H(A1), unq(nonce-value);H(A2)), where A1 comprises unq(username):realm:password and

A2 comprises the uri, p. 11, §3.2.2, p. 13, §3.2.2.1-3.2.2.2 & p. 14, §3.2.2.3) is additionally based on at least one item in the group of time, date and header information (created based on header information, because it is based in part on the username, p. 11, §§3.2.2.1-3.2.2.2, and on time, because the nonce included in the request-digest value, p. 13, §3.2.2.1, is disclosed as being based on a time-stamp, p. 9, §nonce).

Regarding claim 9, Franks discloses determining, in said second device (server), a device-type (username of device's user, p. 17, §3.3, ¶1) of said first device based on said first header information (response), creating a second signature (performing the same digest operation, p. 17, §3.3, ¶1) in said second device (server performs the same digest operation) based on at least tamper-resistant information associated with said determined device-type (password associated with username) and accepting said determined device-type (device is used by user having username) as authentic if said first and second signatures agree (compare the result, p. 17, §3.3, ¶1 & see p. 4, last paragraph for the server accepting/not accepting a response).

Regarding claim 12, Franks discloses a communication device (client) connectable to a communications system (communication system through which the client requests, p. 11, §3.2.2, ¶1 and the server receives requests, p. 8, §3.2.1, ¶1) comprising means (client) for providing a first header information (components 'username|realm|nonce|digest-uri', p. 11, §3.2.2) of a communication message (HTTP request, p. 6, §3.1.1, ¶1, p. 7, §3.2.1, ¶1 & p. 11, §3.2.2, ¶1), said first header information (username|realm|nonce|digest-uri) being related with a device-type associated commitment (including the username shows the device is associated with the user, p. 11, §3.2.2, ¶1), tamper-resistant storage of device-type specific information (A1, including hashed username and password, p. 13, definition of A1) of said communication device (A1 is created using a hash function to create a signature, which is tamper resistant because to create the hash, the password must be known), a tamper-resistant signature generator (client), arranged to create a first signature (response, which comprises H(H(A1), unq(nonce-value);H(A2)), where A1 comprises unq(username):realm:password and A2 comprises the uri, p. 11, §3.2.2, p. 13, §3.2.2.1-3.2.2.2 & p. 14, §3.2.2.3) based on at least said device-type specific information (result of hash function is based on username and password, see definition of A1 on p. 13, §3.2.2.2), means (client) for providing second header information (Authorization header is created by client, p. 11, §3.2.2, ¶1) of said communication message (HTTP request, p. 11, §3.2.2, ¶1) comprising said signature (the request contains the response, see §3.2.2, definition of digest-response) and communication means (client) communicating said communication message (HTTP request) to another device (server) connected to said communication system (HTTP request with authorization header is sent to the server from the client, p. 17, §3.3, ¶1).

Regarding claim 13, Franks discloses wherein said communication means is arranged to support a transfer protocol selected from the group of HyperText Transfer Protocol (HTTP/1.0, p. 6, §3.1.1, ¶1).

Regarding claim 15, Franks discloses wherein said first device is a user terminal (receives user's username and password, p. 8, §3.2.1, definition of 'realm').

Regarding claim 16, Franks discloses a communication device (server) connectable to a communication system (communication system through which the client requests, p. 11, §3.2.2, ¶1 and the server receives requests, p. 8, §3.2.1, ¶1) comprising communication means for receiving a communication message (HTTP request comprising an authorization header, p. 6, §3.1.1, ¶1, p. 7, §3.2.1, ¶1 & p. 11, §3.2.2, ¶1) from a sending device connected to said communication system (client, HTTP request with authorization header is sent to the server from the client, p. 17, §3.3, ¶1), said communication message (HTTP request) comprising a first header information (components 'username|realm|nonce|digest-uri', p. 11, §3.2.2) being related with a device-type associated commitment (including the username shows the device is associated with the user, p. 11, §3.2.2, ¶1), said communication message (HTTP request) further comprising second header information (Authorization header is created by client, p. 11, §3.2.2, ¶1) in turn comprising a first signature (response, which comprises H(H(A1), unq(nonce-value);H(A2)), where A1 comprises unq(username):realm:password and A2 comprises the uri, p. 11, §3.2.2, p. 13, §3.2.2.1-3.2.2.2 & p. 14, §3.2.2.3) and authenticating means (server) arranged to verify said first signature (verifies response; server performs the same digest operation performed by the client, and compares the result to the given request-digest value, p. 17, §3.3, ¶1).

Regarding claim 17, Franks discloses wherein said authentication means (server) in turn comprises means for determining a device-type (who is using the device) of said sending device (client) based on said first header information (server determines password corresponding to the username submitted in the request), storage of device-type specific information of communication devices (the server must have available at least H(A1) which is a hash of at least the username and password at the time of re-creating the digest; see p. 17, §3.3, ¶2 for storing at least H(A1), ¶1 for performing the same digest and p. 13, §3.2.2.2 for the definition of A1; p. 26, §4.13, ¶1), a signature generator (server) arranged to retrieve device-type specific information (at least H(A1)) corresponding to said determined device-type (who is using the device), said signature generator being further arranged to create a second signature (perform the same digest operation, p. 17, §3.3, ¶1) based on said retrieved device-type specific information (H(A1) is used to create the original digest and hence used to create the second digest, p. 17, §3.3, ¶¶1-2) and means for accepting said determine device-type as authentic if said first and second signatures agree (server performs the same digest operation performed by the client, and compares the result to the given request-digest value, p. 17, §3.3, ¶1).

Regarding claim 19, Franks discloses wherein said communication means (server) is based on a transfer protocol selected from the group of HyperText Transfer Protocol (HTTP/1.0, p. 6, §3.1.1, ¶1).

Regarding claim 21, Franks discloses wherein said communication device is a server (server, p. 17, §3.3, ¶1).

Claim Rejections - 35 USC § 103

9. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

10. Claims 10 & 18 are rejected under 35 U.S.C. 103(a) as being unpatentable over **Franks**, as applied to claim 1 & 16 above, in further view of U.S. Patent 5,841,970 to **Tabuki**.

Regarding claim 10, Franks lacks forwarding information about said first header information and said first signature from said second device to a third device, requesting a verification of the authenticity of said first header information by said third device and accepting said first header information as authentic if said third device provides a positive verification. However, Tabuki teaches a system where an application server receives a request for authentication (col. 4, lines 10-14), forwards authentication information and identification information to a verification server, requesting a verification of the authentication information and identification information (col. 4, lines 19-22) and accepts the authentication information and identification information as authentic if the verification server provides a positive verification (col. 4, lines 33-37). This is useful to free the application server from the need to keep valid authentication data for the authentication of user hosts (col. 3, lines 44-49). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Franks to further include the steps of forwarding information about said first header information and said first signature (identification and authentication information) from said second device (Franks' server) to a third device (a verification server), requesting a verification of the authenticity of said first header information by said third device (Franks' server requesting verification of the signature) and accepting said first header information as authentic if said third device provides a positive verification. One of ordinary skill in the art would have been motivated to perform such a modification to free Franks' server from having to store information about the users that is needed for verification, such as the user's passwords and usernames, as taught by Tabuki.

Regarding claim 18, Franks lacks means for forwarding information about said first header information and said first signature from said second device to a further device, means for requesting a verification of the authenticity of said first header information by said further device and means for accepting said first header information as authentic if said third device provides a positive verification. However, Tabuki teaches a system where an application server receives a request for authentication (col. 4, lines 10-14), forwards authentication information and identification information to a verification server, requesting a verification of the authentication information and identification information (col. 4, lines 19-22) and accepts the authentication information and identification information as authentic if the verification server provides a positive verification (col. 4, lines 33-37). This is useful to free the application server from the need to keep valid authentication data for the authentication of user hosts (col. 3, lines 44-49). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Franks' server to include the functionality of Tabuki's application server, and as such to further include means (application server) for forwarding information about said first header information and said first signature (identification and authentication information) from said second device (Franks' server) to a third device (a verification server), means (application server) for requesting a verification of the authenticity of said first header information by said third device (Franks' server requesting verification of the signature) and means (application server) for accepting said first header information as authentic if said third device provides a positive verification. One of ordinary skill in the art would have been motivated to perform such a modification to free Franks' server from having to store information about the users that is needed for verification, such as the user's passwords and usernames, as taught by Tabuki.

Allowable Subject Matter

11. Claims 3, 11, 14 & 20 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

12. The following is a statement of reasons for the indication of allowable subject matter:

c. Regarding claims 3, 14 & 20, the prior art of record fails to teach or disclose, either alone or in combination, wherein said device-type associated commitment is a commitment to follow Digital Rights Management compliance, in combination with the other elements of the claims. Franks' header includes information on which user is using the device, but not DRM compliance. Further, it is known that HTTP messages can include a UserAgent information in a header, but the UserAgent information (often the browser) is not a commitment to DRM compliance. U.S. Patent 6,799,197 to Shetty et al. is cited for teaching the posting of configuration data to a server (col. 9). This is sent as a separate message, rather than as a header to a communications message with a signature. U.S. Patent Application Publication 2003/0014496 to Spencer et al. teaches receiving information about the capability and type of playback device, but does not disclose a header. U.S. Patent Application Publication 2006/0150257 to Leung et al. teaches receiving a digital certificate of a client (¶132) and a version of the black box (DRM) software (¶125) of a client, but lacks including these in a header. Further, Leung lacks information that ties the black box to, for example, a browser that would imply browser information is a commitment to DRM compliance, because in Leung, the black box is necessarily a separate and trusted component. There is insufficient evidence to support the feasibility of including any of the above information in Franks' authorization header, due to size constraints and the fact that Franks' header only specifies the user who is using a device, but no more information about the device-type.

d. Regarding claim 11, the prior art of record fails to teach or disclose, either alone or in combination, wherein said third device is associated with a manufacturer of said first device, in combination with the other elements of the claim. The applied reference to Tabuki discloses performing authentications for various clients, but is silent regarding the association between the verification server and the client requesting access to the application server. U.S. Patent 6,510,236 to Crane et al. teaches a system of offloading authentication duties to another server, but is also silent regarding the manufacturer of the first device being the authenticator.

Conclusion

13. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

e. U.S. Patent Application Publication 2003/0097564 to Tewari et al. is cited for teaching sending a URL including a hash value created using a secret key, current time and other parameters (¶610).

f. U.S. Patents 5,740,361 and 6,487,667 to Brown are cited for teaching the use of an authentication deity for performing authentication services on behalf of another entity controlling access to resources.

g. "Profiles for the Situated Web" by Suryanarayana et al. is cited for teaching using HTTP headers to convey user agent and device capability information.

14. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Michael J. Simitoski whose telephone number is (571) 272-3841. The examiner can normally be reached on Monday - Thursday, 6:45 a.m. - 4:15 p.m..

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kambiz Zand can be reached on (571) 272-3811. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

October 15, 2007
Michael J. Simitoski
/Michael J. Simitoski/